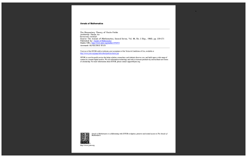
# Decidability of the class of all $\mathbb{Z}/_{m}\mathbb{Z}$:
# A Problem of Ax

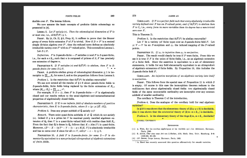
Jamshid Derakhshan (Oxford)
Joint work with Angus Macintyre (Edinburgh)



$\mathcal{L}_{rings} = \{+, \cdot, 0, 1\}$

Formulas : $p(x_1,\dots,x_n)=0 \wedge q(x_1,\dots,x_n)\neq 0$, $p,q\in\mathbb{Z}[x_1,\dots,x_n]$

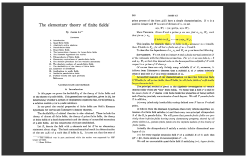
Sentences : $-1$ is a square, $\forall x \exists y \ x=y^2$



An $\mathcal{L}$-structure $M$ is DECIDABLE if given an $\mathcal{L}$-sentence $\sigma$ there is an algorithm (Turing machine) that would determine whether $\sigma$ holds in $M$.

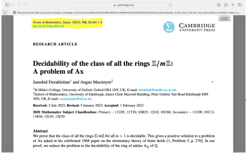
By Ax the class $\mathcal{C}=\{\mathbb{Z}/_{p^k}\mathbb{Z} : p \text{ prime}, k\geq 1\}$ is decidable.

BUT THERE IS NO WAY TO DEDUCE FROM THIS AX'S PROBLEM DIRECTLY:



We can deduce decidability of the class of products of members of $\mathcal{C}$, since $\mathbb{Z}/_{m}\mathbb{Z} \simeq \mathbb{Z}/_{p_1^{k_1}}\mathbb{Z}\times\cdots\times\mathbb{Z}/_{p_r^{k_r}}\mathbb{Z}$ if $m=p_1^{k_1}\cdots p_r^{k_r}$ but this is larger than the class $\{\mathbb{Z}/_{m}\mathbb{Z} : m>1\}$ since it contains repeated products of members in $\mathcal{C}$.

**Theorem.** The problem of Ax has a positive solution, ie. given a sentence $\sigma$ from the language of rings, it is possible to decide whether $\sigma$ holds in $\mathbb{Z}/_{m}\mathbb{Z}$ for all $m>1$.



*Forum of Mathematics, Sigma* (2023), **Vol. 11**:e64 1–6
doi:10.1017/fms.2023.62

CAMBRIDGE UNIVERSITY PRESS

RESEARCH ARTICLE

## Decidability of the class of all the rings $\mathbb{Z}/m\mathbb{Z}$: A problem of Ax

Jamshid Derakhshan[1] and Angus Macintyre[2]

[1]St Hilda's College, University of Oxford, Oxford OX4 1DY, UK; E-mail: derakhsh@maths.ox.ac.uk.
[2]School of Mathematics, University of Edinburgh, James Clerk Maxwell Building, Peter Guthrie Tait Road Edinburgh EH9 3FD, UK; E-mail: a.macintyre@ed.ac.uk.

**Received:** 2 July 2022; **Revised:** 5 January 2023; **Accepted:** 1 February 2023

**2020 Mathematics Subject Classification:** *Primary* – 11U05, 11T30, 03B25, 12J10, 03C60; *Secondary* – 11U09, 03C13, 11R56, 12L05, 12E30

**Abstract**

We prove that the class of all the rings $\mathbb{Z}/m\mathbb{Z}$ for all $m>1$ is decidable. This gives a positive solution to a problem of Ax asked in his celebrated 1968 paper on the elementary theory of finite fields [1, Problem 5, p. 270]. In our proof, we reduce the problem to the decidability of the ring of adeles $\mathbb{A}_{\mathbb{Q}}$ of $\mathbb{Q}$.

Recall If $M$ is an $\mathcal{L}$-structure and $\phi(x_1,\dots,x_n)$ an $\mathcal{L}$-formula, the set $\phi(M)=\{(a_1,\dots,a_n)\in M^n \mid M\models\phi(x_1,\dots,x_n)\}$ is called ($\mathcal{L}$-) definable.

A function $M^k \to M$ is $(\mathcal{L}\text{-})$definable if graph$(f)$ is $(\mathcal{L}\text{-})$ definable.

Examples. $GL_n(K)$, $K$ a field (in $\mathcal{L}_{rings}$)

Solutions in $K^n$ of polynomial equations

Definability is preserved by taking complements

Boolean combinations, and projections

$$M^{n+k} \xrightarrow{\pi_n} M^n$$

Solution to Ax's problem came from model theory of adeles. Angus Macintyre and myself have been developing some works on this for the last 15+ years.

## $\boxed{\text{Adeles}}$

A global field is either a number field, i.e., a finite extension of $\mathbb{Q}$ or a global function field, i.e., a function field of a curve over a finite field $\mathbb{F}_q$.

Adeles are locally compact rings associated to global fields. So we have $\mathbb{A}_K$ for any global field $K$.

$\left\{\begin{matrix}\text{A. Weil} \\ \sim 1943\end{matrix}\right\}$ $\left\{\begin{matrix}\text{E. Artin} \\ \sim 1943\end{matrix}\right\}$

- RH for curves $V(\mathbb{F}_q)$
- Zeta functions Tate $\underline{1950}$

$\mathbb{A}_K^{\times} = I_K$

Chevalley $\underline{\underline{\sim 1937}}$

In this talk, and for the solution of Ax's problem we only need $\mathbb{A}_{\mathbb{Q}}$.

Recall that an absolute value on a field $K$ is a function $|\cdot| : K \longrightarrow \mathbb{R}_{\geq 0}$ s.t. $|x| \geq 0$ and $|x| = 0 \Leftrightarrow x = 0$

- $|xy| = |x||y|$, $\underline{|x+y| \leq |x| + |y|}$

if $\underline{|x+y| \leq \max\{|x|, |y|\}}$, $|\cdot|$ is non-archimedean.

Examples.
- Trivial valuation ($|a| = 1$ for all $a \neq 0$, $|0| = 0$). ←
- The ordinary absolute value on $\underline{\mathbb{Q}}$, denoted $\underline{|\cdot|_\infty}$.
- For any prime $p$, the $p$-adic absolute value denoted $|\cdot|_p$

defined as $\underline{|\alpha|_p = p^{-v_p(\alpha)}}$, where for $\alpha \in \mathbb{Q}$

$v_p(\alpha) = r$ if $\alpha$ can be written as $\underline{p^r \frac{m}{n}}$ where $m, n \in \mathbb{Z}$ are not divisible by $p$.

An absolute value induces a distance $\underline{d(\alpha,\beta) = |\alpha - \beta|}$ on $\underline{\mathbb{Q}, \text{ hence a topology}}$.

By a $\underline{\text{theorem of Ostrowski}}$ $\boxed{V_{\mathbb{Q}} = \{ |\cdot|, |\cdot|_p : p \text{ prime} \}}$ are all the non-trivial absolute values on $\mathbb{Q}$ up to equivalence.

The completion of $\mathbb{Q}$ with respect to $|\cdot|$ is $\mathbb{R}$, and the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$ is the p-adic numbers $\underline{\underline{\mathbb{Q}_p}}$.

$\mathbb{Q}_p$ is locally compact, hence carries a Haar measure.

$\mathbb{Z}_p = \underline{\{ x \in \mathbb{Q}_p : |x|_p \le 1 \}}$ is the ring of p-adic integers which is a local ring with unique maximal ideal

$M_p = \{ x \in \mathbb{Q}_p : \underline{|x|_p} < 1 \}$ and residue field $\underline{\mathbb{F}_p = \mathbb{Z}_p / M_p}$.

We set $\boxed{\mathbb{R} = \mathbb{Q}_\infty}$. $\mathbb{Q}_p$

The ring of $\boxed{\text{adeles of } \mathbb{Q}}$ is the subring (with componentwise operations) of the direct product $\boxed{\prod_{p \le \infty} \mathbb{Q}_p}$ defined by

$$\underline{\mathbb{A}_{\mathbb{Q}}} = \left\{ \underline{\boxed{(x(p))_p}} \in \prod_{p \le \infty} \mathbb{Q}_p \;\Big|\; \underline{\boxed{x(p) \in \mathbb{Z}_p}} \text{ for all but finitely many } p \in V_{\mathbb{Q}} \right\}$$

$$\mathbb{A}^{\text{fin}}_{\mathbb{Q}} = \left\{ \underline{(x(p))_p} \in \underline{\prod_{p < \infty} \mathbb{Q}} \;\Big|\; \boxed{x(p) \in \mathbb{Z}_p} \text{ for all but finitely many } p \right\}$$

is the ring of finite adeles of $\mathbb{Q}$.

$\mathbb{A}_{\mathbb{Q}}$ and $\mathbb{A}^{\text{fin}}_{\mathbb{Q}}$ are locally compact and carry Haar measures.

$\underline{\text{Theorem 1.}}$ ( Derakhshan - Macintyre $\underline{\text{2022 APAL}}$ )

$\mathbb{A}_K$ has a quantifier-elimination in $\mathcal{L}^{*} =$ def exl drcig

$\underline{\text{Cor.}}$ $\boxed{\mathbb{A}_K \text{ is decidable}}$ ( proved first by V. Weispfenning 1978 unpublished ).

$\boxed{\text{The Boolean Algebra}}$

Language of Boolean alg $\underline{\{\wedge, \vee, \neg, 0, 1\}}$. The set of idempotents

$\mathbb{B}_{\mathbb{Q}} = \{ a \in \mathbb{A}_{\mathbb{Q}} \mid a = a^2 \}$ forms a Boolean alg

with operation

$(0, 1, 0, \dots, 1 \dots)$

$$e \wedge f = ef$$

$$e \vee f = 1 - (1-e)(1-f) = e + f - ef$$

$$\neg e = 1 - e$$

$(1, \dots 1)$ $\underline{1}$ top. $\underline{\underline{0}}$ $(0, 0, \dots)$

Carries a partial order $\underline{e \leq f} \Leftrightarrow \underline{\underline{ef = e}}$.

An idempotent is called $\underline{\text{minimal}}$ if it is $\underline{\text{non-zero}}$ and $\underline{\text{minimal}}$ with respect to this order.

$(0, \dots, 1, 0 \dots)$

Let atom$(x)$ express $x$ is minimal idempotent

There is a bijective correspondence between subsets of $\underline{|\{|\cdot|_\infty, |\cdot|_p, \dots\}|}$ $\underline{V_{\mathbb{Q}}}$ and idempotents in $\underline{\underline{\mathbb{A}_{\mathbb{Q}}}}$ given by:

$$V_{\mathbb{Q}} \supseteq \underline{\underline{X}} \longrightarrow \underline{\underline{e_X}} \in B_{\mathbb{Q}} \qquad e_X(p) = \begin{cases} 1 & \text{if } p \in X \\ 0 & \text{if } p \notin X \end{cases}$$

$$X = \{\underbrace{p}\,/\,\underbrace{a(p)} \neq 0\} \longleftarrow \textcircled{e}$$

$$e = e_X$$

The support of $a \in \mathbb{A}_{\mathbb{Q}}$ denoted supp$(a)$ is defined to be

$$\text{supp}(a) = \{ p \in V_{\mathbb{Q}} \mid a(p) \neq 0 \}.$$

Theorem 2. (Derakhshan – Macintyre APAL 2022).

The set of elements of $B_{\mathbb{Q}}$ with finite support $\boxed{\text{Fin}_{\mathbb{Q}}}$ is an $\mathcal{L}_{\text{rings}}$-definable subset of $\underline{\underline{\mathbb{A}_{\mathbb{Q}}}}$.

$\boxed{\text{Boolean Values}}$

**Lemma:** If $\phi(x_1, \dots, x_n)$ is an $\mathcal{L}_{rings}$-formula. There is an $\mathcal{L}_{rings}$ definable function

$$\left(\mathbb{A}_{\mathbb{Q}}^{fin}\right)^n \longrightarrow \mathbb{B}_{\mathbb{Q}}^{fin}$$

$$(a_1, \dots, a_n) \longmapsto \boxed{[\![ \phi(a_1, \dots, a_n) ]\!]}^{fin}$$ defined as the sup of all non-archimedean minimal idempotents $e$ s.t. $\boxed{e\mathbb{A}_{\mathbb{Q}}^{fin}} \models \phi(ea_1, \dots, ea_n)$

$\prod_{i \in I} M_i$ $\quad \phi(\bar{x})$ $\quad [\![ \phi(\bar{a}) ]\!] = \{ i \in I \mid M_i \models \phi(a(i)) \}$

$\mathbb{A}_{\mathbb{Q}}$

$\mathbb{A}_K$

$\left( e\mathbb{A}_{\mathbb{Q}}^{fin} \simeq \mathbb{Q}_p \quad ea \longmapsto a(p) \right.$ where $e$ supported at $p$ )

## Uniform Definition of Valuation rings

**Theorem 3.** Cluckers - Derakhshan - Leenknegt - Macintyre APAL 2014)

There is an $\mathcal{L}_{rings}$-formula ($\exists\forall$) which uniformly defines the valuation ring of all Henselian valued fields with finite or pseudo-finite residue field

$\mathbb{A}_{\mathbb{F}_q(t)})$

**Cor.** There is an $\mathcal{L}_{rings}$-formula $\boxed{\Phi_{val}(x)}$ which defines all $\mathbb{Z}_p$ in $\mathbb{Q}_p$.

( Julia Robinson's def of $\mathbb{Z}_p$ had $p$ as parameter)

## Solution of Ax's Problem

**Part I**

By Theorem 3 on uniform definability of $\mathbb{Z}_p$ in $\mathbb{Q}_p$ for $p < \infty$ using $\Phi_{val}(x)$ the set of elements of $\mathbb{A}_{\mathbb{Q}}$ whose $\mathbb{Q}_p$-component is in $\mathbb{Z}_p$ for each $p < \infty$ is definable since it equals

$$\{ a \in \mathbb{A}_{\mathbb{Q}} \mid [\![ \Phi_{val}(a) ]\!]^{fin} = e_{fin} \}$$

$e_{fin}$ = sup of all idempotents supported on all $p < \infty$.

This set is isom to $\mathbb{R} \times \hat{\mathbb{Z}}$.

Consider a positive integer $m = \prod_j q_j^{r_j}$ (coprime prime powers)

Consider the element $g$ which takes value $1$ at all min. idemp's (incl. $\infty$) except those corresponding to the $q_j$'s, and takes value $q_j^{r_j}$ at $q_j$.

(incl. = corresp)

$g-1$ has finite support (all conditions are $\mathcal{L}_{\text{rings}}$-def)

The quotient $\mathbb{R} \times \hat{\mathbb{Z}} / (g)$ isom $\prod_j \mathbb{Z}_{q_j} / q_j^{r_j} \mathbb{Z}_{q_j} \simeq \prod_j \mathbb{Z} / q_j^{r_j} \mathbb{Z}$

$$\simeq \mathbb{Z}/m\mathbb{Z}$$

The set all such $g$ is definable $\overset{(\mathcal{L}_{\text{rings}})}{}$ in $\mathbb{A}_{\mathbb{Q}}$.

## Part II

Suppose $g-1$ is an element of finite support.

Suppose $g$ takes values in $\mathbb{Z}_p$ for all $p < \infty$ and for some $p < \infty$, $g$ takes value a $p$-adic non-unit.

i.e..

- $g-1 \in \mathcal{F}in_{\mathbb{Q}}$
- $[\![ \Phi_{val}(g) ]\!]^{fin} = e_{fin} \wedge [\![ \Phi_{val}(g) \wedge \neg \Phi_{val}(g^{-1}) ]\!]^{fin} \neq 0$

[ $\mathcal{L}$rings - conditions! ].

$\Rightarrow$ $g$ takes value $1$ at all but finitely many elts of $V_{\mathbb{Q}}$.

Assume $g$ takes value $1$ at the infinite prime.

( def since $\{ h \in \mathbb{A}_{\mathbb{Q}} \mid h(\infty) = 1 \}$ is $\mathcal{L}$rings-def in $\mathbb{A}_{\mathbb{Q}}$).

Now consider $\mathbb{R} \times \hat{\mathbb{Z}} / (g)$. This quotient is a product over finitely many primes $q_j$ of quotients of $\mathbb{Z}_{q_j}$ by the ideal generated by an elt of $\mathbb{Z}_{q_j}$.

When that elt is a unit the quotient is trivial ring and discarded. For at least one prime $q_j$ the elt is not a unit and then generates same ideal as some power of $q_j$.

$\Rightarrow$ As in Part I, $\mathbb{R} \times \hat{\mathbb{Z}} / (g) \simeq \mathbb{Z} / m\mathbb{Z}$. for some $m > 1$.

The assumptions on $g$ are all $\mathcal{L}$rings-def.

Parts I + II $\Rightarrow$ a uniform interpretation of $\mathbb{Z}/m\mathbb{Z}$ in $\mathbb{A}_{\mathbb{Q}}$.

**Part III** The class $\{ \mathbb{Z}/m\mathbb{Z} \mid m>1 \}$ is decidable.

Pf: Let $\mathcal{X}$ denote the set of all $g \in \mathbb{A}_{\mathbb{Q}}$ s.t. $g-1$ has finite support, $g$ takes value $1$ at infinite prime, $g$ takes values in $\mathbb{Z}_p$ $\forall p<\infty$, and $g$ takes as value a $p$-adic non-unit at some $p<\infty$.

By Part 2, $\mathcal{X}$ is $\mathcal{L}_{\text{rings}}$-definable in $\mathbb{A}_{\mathbb{Q}}$.

Part I + Part II $\Rightarrow$ any ring from the class $\{\mathbb{Z}/m\mathbb{Z} \mid m>1\}$ is isom to a ring from the class

$$\{ (\mathbb{R}\times\hat{\mathbb{Z}})/(g) \mid g \in \mathcal{X} \}$$

and conversely any $\mathbb{R}\times\hat{\mathbb{Z}}/(g)$, where $g\in\mathcal{X}$ is isom to

$\mathbb{Z}/m\mathbb{Z}$ for some $m>1$.

Thus deciding whether an $\mathcal{L}_{\text{rings}}$-sentence $\Psi$ holds in $\mathbb{Z}/m\mathbb{Z}$ for all $m>1$ is equivalent to deciding whether $\Psi$ holds in $\mathbb{R}\times\hat{\mathbb{Z}}/(g)$ for all $g\in\mathcal{X}$.

Since $\mathcal{X}$ and $\mathbb{R}\times\hat{\mathbb{Z}}$ are definable in $\mathbb{A}_{\mathbb{Q}}$ this decision procedure can be carried out by the decidability of $\mathbb{A}_{\mathbb{Q}}$.

QED

Ax Problem $\left| \begin{array}{l} \text{definability of Fin } \mathbb{Q} \\ \quad \prod \cdots \mathbb{Z} \text{ fin.} \end{array} \right|$

Reduce Ax Problem to decidability of $\underline{\underline{\mathbb{A}_{\mathbb{Q}}}}$

Follows from QE for $\mathbb{A}_K$.

Reduces to deciding basic sets in QE.

These basic formula can be decided using

- Chebotarev density thm.

AJAC. 2014 2021. QE

## Model theory for restricted product.

$\mathcal{L}$ - lang.
$I$ - index
( ~~$M_f$~~
$(M_i : i \in I)$

Feferman – Vaught 1959. · generalized weak product.

$\left( \prod_{i \in I}^{(\Phi)} M_i \right. \to (a_1, \dots a_i, \dots) \quad M_i \models \phi(a_1(i), \dots a_n(i) \dots) \left. \right)$ $\phi(x)$ $\mathcal{L}_f'$

- QE for such restricted product

$\mathbb{A}_K$.

- ~~$\mathbb{A}_K$~~ $\{ \mathbb{Z}/m\mathbb{Z} : m > 1 \}$

- Derakhshan – Hrushovski
Imaginaries, Products, and the adele rings, arXiv 2023 Sept.

**D**escribe the imaginaries ( quotients by def. eq. relns )

- $\mathbb{C}$
- $\mathbb{R}$.
- ACVF QE. $+ \dots +$ $GL_n(K)$ / $GL_n(\mathcal{O})$

Hrushovski – Haskell – Macpherson. $\boxed{\text{EI ACVF}}$ $\boxed{\text{Geometric Sorts.}}$

Hrushovski – Rideau – Martin. JEMS 2020.

- EI for $\mathbb{Q}_p$ uniformly in $p$. .

$GL_n(\mathbb{Q}_p)/GL_n(\mathbb{Z}_p)$

- M. Hils – S.-R-K.

- EI for $\mathbb{A}_{\mathbb{Q}}$.
$\mathbb{A}_K$.

General thm descr
unary : products of structure. ← local stability thy
" "
Booleanizations

descriptive set thry Borel eq. rel.
Kechris – Harrington.

unif EI $\mathbb{Q}_p$ + unif in p. constants $\mathrm{Gal}(k_n/\mathbb{Q}_p)$

$S_n = GL_n(\mathbb{Q}_p)/GL_n(\mathbb{Z}_p)$

$T_n$

$\mathrm{Fin}(\,[\,q + \bar{a} + \,]\,)$

local. lattice.

Reduced

to def eq.
sorts

reduct

wEI

$S/\sim$